501.43643X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): M. EHAMA et aL

Serial No.: Not Yet Assigned

Filed: March 17, 2004

Title: SECURITY SYSTEM

LETTER CLAIMING RIGHT OF PRIORITY

Mail Stop: Patent Applications
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

March 17, 2004

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicants hereby claim the right of priority based on **Japanese** Patent Application No. **2003**-072919, filed March 18, 2003.

A certified copy of said **Japanese** Application is attached.

Respectfully submitted,
ANTONELLI, TERRY, STOUT & KRAUS, LLP

Paul J. Skwierawski
Registration No. 32,173

PJW/dks
Attachment
(703) 312-6600

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　３月１８日
出願番号 Application Number: [ST. 10/C]:	特願２００３－０７２９１９ [ＪＰ２００３－０７２９１９]
出願人 Applicant(s):	株式会社ルネサステクノロジ

２００３年１２月　４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１００３４３

【書類名】　特許願

【整理番号】　K03001021A

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/14

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　江浜　真和

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　田中　和彦

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　細木　浩二

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　中田　啓明

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】セキュリティシステム

【特許請求の範囲】

【請求項１】

演算を行うプロセッサコアと、外部バスと接続するための外部バスインターフェースと、ローカルメモリへのアクセスを制御するメモリインターフェースと、前記プロセッサコアと前記外部バスインターフェースと前記メモリインターフェースとを接続する内部バスとを有する半導体装置であって、

前記外部バスインターフェースは、前記外部バスからのリクエストを受けるアクセス制御回路と、前記アクセス制御回路に接続され前記外部バスアクセスの可否を判定するＴＬＢと、前記プロセッサコアからの要求によりＴＬＢを書き換えるＴＬＢ制御回路を有し、

前記外部バスからのリクエストを受けたアクセス制御回路は、該リクエストのアドレスが、前記ＴＬＢ内に設定されたアクセス許可範囲内のアドレスか否か問い合わせるＴＬＢ判定信号を前記ＴＬＢへ送信し、

前記ＴＬＢは、前記リクエストのアドレスが、前記ＴＬＢ内に設定されたアクセス許可範囲内のアドレスか否かを検索し、アクセス可否を示すＴＬＢ合否信号をアクセス制御回路へ返答し、

前記アクセス制御回路は、前記ＴＬＢ合否信号がアクセス可であることを示している場合、前記内部バスへアクセスを許可し、前記ＴＬＢ合否信号がアクセス否であることを示している場合、前記リクエストを破棄することを特徴とする半導体装置。

【請求項２】

請求項１記載の半導体装置であって、

前記ＴＬＢ制御回路は、前記プロセッサコアが出力するＴＬＢ更新要求に基づき、前記アクセス可能範囲を変更可能であることを特徴とする半導体装置。

【請求項３】

請求項１記載の半導体装置であって、

前記外部バスは、ＰＣＩバスであることを特徴とする半導体装置。

【請求項４】

請求項１記載の半導体装置であって、

前記外部バスは、汎用バスであることを特徴とする半導体装置。

【請求項５】

請求項１記載の半導体装置であって、

前記内部バスに接続され、暗号処理を行う暗号演算回路をさらに有し、

前記アクセス制御回路は、当該暗号演算回路の秘密鍵や暗号処理方法を決定するレジスタへのアクセスを制限することを特徴とする半導体装置。

【請求項６】

請求項１記載の半導体装置であって、

前記アクセス制御回路は、前記ＴＬＢ合否信号がアクセス可であることを示している場合、前記内部バス、前記メモリインタフェースを介して前記ローカルメモリへのアクセスを許可することを特徴とする半導体装置。

【請求項７】

外部バスに接続された半導体装置におけるバスインターフェース装置であって、前記半導体装置内の内部バスに接続され、

前記外部バスからのリクエストを受けるアクセス制御回路と、前記アクセス制御回路に接続され前記外部バスアクセスの可否を判定するＴＬＢと、前記プロセッサコアからの要求によりＴＬＢを書き換えるＴＬＢ制御回路を有し、

前記外部バスからのリクエストを受けたアクセス制御回路は、該リクエストのアドレスが、前記ＴＬＢ内に設定されたアクセス許可範囲内のアドレスか否か問い合わせるＴＬＢ判定信号を前記ＴＬＢへ送信し、

前記ＴＬＢは、前記リクエストのアドレスが、前記ＴＬＢ内に設定されたアクセス許可範囲内のアドレスか否かを検索し、アクセス可否を示すＴＬＢ合否信号をアクセス制御回路へ返答し、

前記アクセス制御回路は、前記ＴＬＢ合否信号がアクセス可であることを示している場合、前記内部バスへアクセスを許可し、前記ＴＬＢ合否信号がアクセス否であることを示している場合、前記リクエストを破棄することを特徴とするバスインタフェース装置。

【請求項８】

請求項７記載のバスインターフェース装置であって、

外部バスからアクセスされたアドレスを内部バスで用いるためのアドレスに変換するデコーダを有し、

前記アクセス制御回路は、前記デコーダで変換されたアドレスを用いて内部バスへリクエストを送信することを特徴とするバスインターフェース装置。

【請求項９】

請求項７記載のバスインタフェース装置であって、

前記半導体装置内部の所定のアドレス空間がアクセス可能であるかを示す許可ビット群を格納したレジスタと、前記外部からのアクセスが示すアドレスが当該半導体装置内部のアクセス可能な領域のアドレスか否かを判定するアクセス判定装置を有し、

前記アクセス判定回路は、前記デコーダと当該デコーダに接続されたセレクタを備え、

前記デコーダで変換されたアドレスから領域選択信号を生成し、前記許可ビット群のレジスタから出力される許可ビット信号と、前記領域選択信号を比較し、

前記領域選択信号と、前記許可ビット信号とが一致した場合は、アクセスが可であることを示す前記アクセス合否信号を出力し、

前記領域選択信号と、前記許可ビット信号とが一致しない場合は、アクセスが否であることを示す前記アクセス合否信号を出力することを特徴とするバスインタフェース装置。

【請求項１０】

請求項７記載のバスインタフェース装置であって、

前記許可ビット群に格納されたデータの更新を行う許可ビット制御回路をさらに有し、

前記許可ビット制御回路は、内部バスを介して送信される書き換え要求信号に基づき、前記許可ビット群に格納されたデータを変更可能であることを特徴とするバスインタフェース装置。

【請求項１１】

記憶装置が接続された第１の半導体装置、第２の半導体装置、前記第１の半導体装置と前記第２の半導体装置を接続する外部バスとを有するコンピュータシステムであって、

前記第１の半導体装置は、

演算を行うプロセッサコアと、前記外部バスに接続されるための外部バスインターフェースと、前記記憶装置へのアクセスを制御するメモリインターフェースと、前記プロセッサコアと前記外部バスインターフェースと前記メモリインターフェースとを接続する内部バスとを有し、

前記第２の半導体装置から前記記憶装置へのアクセスがあった場合、

前記第１の半導体装置は、該アクセスのアドレスが、当該第１の半導体装置内のＴＬＢに予め設定されたアクセス許可範囲内のアドレスか否かを判断し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれる場合、前記内部バスを介して前記記憶装置へのアクセスを許可し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれない場合、前記アクセスを破棄し前記記憶装置へのアクセスを許可しないことを特徴とするコンピュータシステム。

【請求項１２】

請求項１１記載のコンピュータシステムであって、

前記外部バスインターフェースは、前記外部バスからのリクエストを受けるアクセス制御回路と、前記アクセス制御回路に接続され前記外部バスアクセスの可否を判定するＴＬＢと、前記プロセッサコアからの要求によりＴＬＢを書き換えるＴＬＢ制御回路を有し、

前記外部バスからのリクエストを受けたアクセス制御回路は、該リクエストのアドレスが、前記ＴＬＢ内に設定されたアクセス許可範囲内のアドレスか否か問い合わせるＴＬＢ判定信号を前記ＴＬＢへ送信し、

前記ＴＬＢは、前記リクエストのアドレスが、前記ＴＬＢ内に設定されたアクセス許可範囲内のアドレスか否かを検索し、アクセス可否を示すＴＬＢ合否信号をアクセス制御回路へ返答し、

前記アクセス制御回路は、前記ＴＬＢ合否信号がアクセス可であることを示し

ている場合、前記内部バスへアクセスを許可し、前記ＴＬＢ合否信号がアクセス否であることを示している場合、前記リクエストを破棄することを特徴とするコンピュータシステム。

【請求項１３】

任意の機能を有するモジュールと、外部バスに接続されるための外部バスインターフェースと、前記モジュールと前記外部バスインターフェースとを接続する内部バスとを有する半導体装置であって、

前記外部バスに接続される他の装置から前記モジュールへのアクセスがあった場合、

前記半導体装置は、該アクセスのアドレスが、当該半導体装置内のＴＬＢに予め設定されたアクセス許可範囲内のアドレスか否かを判断し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれる場合、前記内部バスを介して前記モジュールへのアクセスを許可し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれない場合、前記アクセスを破棄し前記記憶装置へのアクセスを許可しないことを特徴とする半導体装置。

【請求項１４】

請求項１３記載の半導体装置であって、

当該半導体装置には記憶装置が接続されており、

前記記憶装置へのアクセスを制御するメモリインターフェースをさらに有し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれる場合、前記内部バス、前記メモリインタフェースを介して前記記憶装置へのアクセスを許可することを特徴とする半導体装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は外部バスインターフェースにてプロセッサ内部の機密情報を保護することのできるマイクロプロセッサに関する。

【０００２】

【従来の技術】

特許文献１では、メモリへのデータアクセスを制限するためにメモリインターフェース回路とメモリの間にセキュリティ回路を設け、正しい手順でメモリアクセスが行われているかを監視している。このセキュリティ回路には鍵アドレスが設けてあり、この鍵アドレスに対応する特定の手順でアクセスが発生することで、メモリ空間へアクセス可能な範囲を拡大したり、予測するメモリアクセスからは使用しないメモリ空間を保護しデータ転送が実行されないようにすることが可能であった。また、メモリ保護機能が解除されていないアドレスに対してのアクセスが発生した場合、読み出されたデータの保障は行われないという提案であった。

【０００３】

【特許文献１】

特開２００１－３０６４００号公報

【０００４】

【発明が解決しようとする課題】

従来は外部メモリ空間のみの保護機能であり、プロセッサ内部メモリのデータに関しては保障されない。また、プロセッサ内部のメモリ空間全てにこの機能を搭載したとすると冗長論理が増大し、プロセッサの肥大化を招いてしまう。

【０００５】

また、メモリ空間に対するアドレスの発行順序によって、メモリ保護の合否をハードウェアで行うため、汎用性に乏しい。

【０００６】

また、保護機能を持たないプロセッサでは、外部バスからプロセッサ内部のレジスタやローカルメモリの読み出しや改変が可能であったため、暗号鍵などの機密データが閲覧されたり、開発したソフトウェアがコピーされてしまう可能性があった。

【０００７】

本発明はこのような問題を鑑みてなされたものであり、プロセッサが外部デバイスと通信する汎用バスを用いた不正アクセス防止を目的とする。

【０００８】

【課題を解決するための手段】

この発明に係るプロセッサは、ＰＣＩバスなどのプロセッサ外部の汎用バスとプロセッサの内部バスの間でデータ転送を制御するアクセス制御装置と、アクセスできる範囲が格納されているＴＬＢと、ＴＬＢの内容を更新するＴＬＢ制御回路を具備する。

【０００９】

プロセッサ内部からのアクセスによってのみＴＬＢを更新するＴＬＢ制御回路によってＴＬＢの内容を更新し、その更新した内容はＰＣＩバスなどのプロセッサ外部の汎用バスからのアクセスによって、アクセス制御回路から参照される。

【００１０】

アクセス制御回路からのリクエストによりＴＬＢはアクセス可能領域であるかどうかをアクセス制御回路へ返答し、その結果によって、内部バスへリクエストを出すか、破棄するかを決定し、プロセッサ内部の機密情報を保護する。

【００１１】

【発明の実施の形態】

本発明の実施例について図面を参照して説明する。図１に本発明を適用したコンピュータシステムの構成例を示す。なお簡略化のため、本発明の適用と直接関係のない部分は省略する。

【００１２】

メインＣＰＵ１と高速バスインターフェースを持つノースブリッジ３へプロセッサバス２を用いて接続する。ノースブリッジ３は主記憶装置５とメモリバス４で接続し、また低速バスインターフェースを持つサウスブリッジ７とブリッジ間接続バス６を用いて接続する。

【００１３】

サウスブリッジ７からＰＣＩバス８へ接続され、ＰＣＩバス８上にメディアプロセッサ１００ａ、１００ｂを２個接続している。各々のメディアプロセッサ１００ａ、１００ｂはそれぞれローカルメモリ２０１ａ、２０１ｂへローカルメモリバス２００ａ、２００ｂを用いて接続する。また、フラッシュメモリ２０３ａ

、２０３ｂへフラッシュメモリバス２０２ａ、２０２ｂを用いて接続する。尚、本実施例のメディアプロセッサ及びそれに相当する部分は１チップで構成されるが、複数チップにて実現することも可能である。

【００１４】

メディアプロセッサ１００ａ内部は内部バス１０９を用いて、演算を行うプロセッサコア１０１、ＰＣＩバス８と接続するためのＰＣＩバスインターフェース１０２、プロセッサコア１０１の演算補助を行うコプロセッサ１０３、ローカルメモリへのアクセスを制御するメモリインターフェース１０４、I/Oインターフェースを制御するＩ／Ｏインターフェース１０５、暗号処理を行う暗号処理演算回路１０８が接続されている。暗号処理としては、Multi2/DES等がある。また、コプロセッサ１０３にコプロセッサ用メモリバス１０７を用いてコプロセッサ用メモリ１０６へ接続されている。

【００１５】

さらに、ＰＣＩバスインターフェース１０２は動作設定を行うためのＰＣＩバスインターフェースＰＩＯレジスタ１１６を、プロセッサコア１０１はプロセッサコアＰＩＯレジスタ１１７を、コプロセッサ１０３はコプロセッサＰＩＯレジスタ１１８を、メモリインターフェース１０４はメモリインターフェースＰＩＯレジスタ１１９を、Ｉ／ＯインターフェースＰＩＯレジスタ１２０を、暗号処理演算回路１０８は暗号処理演算回路ＰＩＯレジスタ１２１を、それぞれ持っている。

【００１６】

メディアプロセッサ１００ａのブート時、Ｉ／Ｏインターフェース１０５がフラッシュメモリ２０３ａからプログラムをロードし、内部バス１０９を通してプロセッサコア１０１がそのプログラムを実行することで、まずＰＣＩバスインターフェース１０２内のＴＬＢ制御回路１１２へＴＬＢ書き換えリクエストを発生する。そのリクエストに応じてＴＬＢ制御回路１１２はＴＬＢ更新信号１１５をＴＬＢ１１１へ出すことでＴＬＢ１１１内部を変更し、起動時アクセス可能であったプロセッサ内部と、メディアプロセッサ１００ａの持つローカルメモリ２０１ａとフラッシュメモリ２０３ａの全領域のうち、ある特定の領域のみをアクセ

スできるようにする。

【００１７】

メインＣＰＵ１からメディアプロセッサ１００ａへのリードアクセスが発生した場合には、そのリクエスト信号はノースブリッジ３、サウスブリッジ７へと送られ、ＰＣＩバス８を通してメディアプロセッサ１００ａ内部のＰＣＩバスインターフェース１０２が受ける。リクエスト信号を受けたアクセス制御回路１１０は、リードするアドレスがアクセス可能であるかどうかをＴＬＢ１１１へＴＬＢ判定信号１１３を通して問い合わせる。その信号を受け取ったＴＬＢ１１１は設定されているアドレスと比較し、その合否をＴＬＢ合否信号１１４を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合、内部バス１０９へリクエストを出し、目的のデータを引き出し、ＰＣＩバス８を通してサウスブリッジ７、ノースブリッジ３を経由しメインＣＰＵへとデータを返す。しかし、アクセスできない領域へのリードリクエストであった場合にはアクセス制御回路１１０は不定のデータをメインＣＰＵ１へ返す。

【００１８】

また、ライトリクエストがメインＣＰＵ１からメディアプロセッサ１００ａへ出された場合、リードリクエストと同じ経路でＰＣＩバスインターフェース１０２へと送られる。ライトリクエストを受け取ったアクセス制御回路１１０は、ライトするアドレスがアクセス可能であるかどうかをＴＬＢ１１１へＴＬＢ判定信号１１３を通して問い合わせる。その信号を受け取ったＴＬＢ１１１は内部のアドレスと比較し、その合否をＴＬＢ合否信号１１４を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合であり、内部バス１０９へリクエストを出し、書き換えを行う。しかし、アクセスできない領域へのライトリクエストであった場合にはアクセス制御回路１１０はその要求を破棄する。

【００１９】

さらに、他のＰＣＩデバイスであるメディアプロセッサ１００ｂからのリードリクエストやライトリクエストも、メインＣＰＵ１からのアクセスと同様に判定が行われアクセス制限が行われる。

【００２０】

特に、ＴＬＢ１１１の変更はプロセッサコア１０１からのみ変更可能であり、メインＣＰＵ１や他のＰＣＩデバイスからの変更は一切行うことができない。

【００２１】

図２は汎用バスインターフェース１２３を持つメディアプロセッサ１２６の構成図である。汎用バスインターフェースとはアドレスバスとデータバス、リクエストなどの制御信号を持つバスである。リードリクエストとアドレスを発行することでデータバスに、要求したアドレスのデータを得ることができ、また、ライトリクエストとアドレスを発行し、データバスに書き込むデータを送信することで、変更するアドレスのデータを書き換えることができる。

メディアプロセッサ１２６は内部バス１０９を持ち、その内部バス１０９にプロセッサコア１０１、コプロセッサ１０３、メモリインターフェース１０４、Ｉ／Ｏインターフェース１０５、暗号処理演算回路１０８、汎用バスインターフェース１２３が接続されている。コプロセッサ１０３はコプロセッサ用メモリバス１０７を用いてコプロセッサ用メモリ１０６へ接続、メモリインターフェース１０４はローカルメモリバス２００を用いてローカルメモリ２０１へ接続、Ｉ／Ｏインターフェース１０５はフラッシュメモリバス２０２を用いてフラッシュメモリ２０３へ接続している。

【００２２】

さらに、汎用バスインターフェース１２３は動作設定を行うための汎用バスインターフェースＰＩＯレジスタ１１６を、プロセッサコア１０１はプロセッサコアＰＩＯレジスタ１１７を、コプロセッサ１０３はコプロセッサＰＩＯレジスタ１１８を、メモリインターフェース１０４はメモリインターフェースＰＩＯレジスタ１１９を、Ｉ／Ｏインターフェース１０５はＩ／ＯインターフェースＰＩＯレジスタ１２０を、暗号処理演算回路１０８は暗号処理演算回路ＰＩＯレジスタ１２１を、それぞれ持っている。

【００２３】

メディアプロセッサ１２６がブートすることで、フラッシュメモリ２０３からＩ／Ｏインターフェース１０５がブートプログラムを内部バス１０９を通してプ

ロセッサコア１０１へ送る。そのプログラムによってプロセッサコア１０１より内部バス１０９を用いてＴＬＢ制御回路１１２へＴＬＢ書き換えリクエストを発生し、汎用バスインターフェース１２３内のＴＬＢ１１１を更新する。その更新によって、起動時アクセス可能であったプロセッサ内部と、メディアプロセッサ１０２の持つローカルメモリ２０１とフラッシュメモリ２０３の全領域のうち、ある特定の領域のみをアクセスできるようにする。

【００２４】

汎用バス１２２を用いてメディアプロセッサ１２６と通信を行う汎用プロセッサ１２５は汎用プロセッサ用フラッシュメモリ１２７を汎用プロセッサ用フラッシュメモリバス１２８を用いて接続されており、また汎用プロセッサ用ローカルメモリ１２９と汎用プロセッサ用ローカルメモリバス１３０を用いて接続している構成である。この汎用プロセッサ１２５からメディアプロセッサ１２６へのリードリクエストによりアクセス制御回路１２４が、リードするアドレスがアクセス可能であるかどうかをＴＬＢ１１１へＴＬＢ判定信号１１３を通して問い合わせる。その信号を受け取ったＴＬＢ１１１は設定されているアドレスと比較し、その合否をＴＬＢ合否信号１１４を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合、内部バス１０９へリクエストを出し、目的のデータを引き出し、汎用バス１２２を通して汎用プロセッサ１２５へ返答する。

【００２５】

また、ライトリクエストが汎用プロセッサ１２５からメディアプロセッサ１２６へ出された場合、リードリクエストと同様にアクセス可能領域であるかどうかを判定する。判定の結果、アクセス可能である場合には内部バス１０９を通して目的のアドレスを書き換えるが、アクセス禁止領域の場合にはライトデータは書き込まれず破棄される。

【００２６】

特に、ＴＬＢ１１１の変更はプロセッサコア１０１からのみ変更可能であり、汎用プロセッサ１２５からの変更は一切行うことができない。

【００２７】

演算専用のデジタルシグナルプロセッサ（以下ＤＳＰ）１３１に本発明を採用した実施例を図３に示す。

【００２８】

ＤＳＰ１３１は、内部バス１０９を持ち、その内部バス１０９に演算を行うプロセッサコア１０１、メモリインターフェース１０４、Ｉ／Ｏインターフェース１０５、汎用バスインターフェース１２３が接続されている。メモリインターフェース１０４はローカルメモリバス２００を用いてローカルメモリ２０１へ接続、Ｉ／Ｏインターフェース１０５はフラッシュメモリバス２０２を用いてフラッシュメモリ２０３へ接続している。

【００２９】

汎用バスインターフェース１２３は動作設定を行うための汎用バスインターフェースＰＩＯレジスタ１１６を、プロセッサコア１０１はプロセッサコアＰＩＯレジスタ１１７を、メモリインターフェース１０４はメモリインターフェースＰＩＯレジスタ１１９を、Ｉ／Ｏインターフェース１０５はＩ／ＯインターフェースＰＩＯレジスタ１２０を、それぞれ持っている。

【００３０】

汎用バスインターフェース１２２にはホストＣＰＵとなる汎用プロセッサ１２５が接続されており、その汎用プロセッサ１２５には汎用プロセッサ用フラッシュメモリ１２７が汎用プロセッサ用フラッシュメモリ１２８を用いて接続され、また汎用プロセッサ用ローカルメモリ１２９が汎用プロセッサ用ローカルメモリバス１３０を用いて接続されている。この汎用プロセッサ１２５から、通常全てのＤＳＰ１３１内部へアクセスすることが可能であり、このとき、ＤＳＰ１３１は汎用プロセッサフラッシュメモリからプログラムをロードしてブートし、ＤＳＰ１３１の初期設定もあわせて行う。初期設定が完了し、ＤＳＰ１３１は内部バス１０９から、Ｉ／Ｏインターフェース１０５を通してフラッシュメモリ２０３から汎用バスインターフェース１２３内のＴＬＢ１１１の設定を行う。プロセッサコア１０１からのＴＬＢ書き換えリクエストを受けたＴＬＢ制御回路１１２はＴＬＢ更新信号１１５をＴＬＢ１１１へ出すことでＴＬＢ１１１内部を変更し、起動時にアクセス可能であったＤＳＰ内部と、ＤＳＰ１３１の持つローカルメモ

リ２０１とフラッシュメモリ２０３の全領域のうち、ある特定の領域のみをアクセスできるようにする。

【００３１】

この汎用プロセッサ１２５からＤＳＰ１３１へのリードリクエストによりアクセス制御回路１２４が、リードするアドレスがアクセス可能であるかどうかをＴＬＢ１１１へＴＬＢ判定信号１１３を通して問い合わせる。その信号を受け取ったＴＬＢ１１１は設定されているアドレスと比較し、その合否をＴＬＢ合否信号１１４を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合、内部バス１０９へリクエストを出し、目的のデータを引き出し、汎用バス１２２を通して汎用プロセッサ１２５へ返答する。

【００３２】

また、ライトリクエストが汎用プロセッサ１２５からＤＳＰ１３１へ出された場合、リードリクエストと同様にアクセス可能領域であるかどうかを判定する。判定の結果、アクセス可能である場合には内部バス１０９を通して目的のアドレスを書き換えるが、アクセス禁止領域の場合にはライトデータは書き込まれず破棄される。

【００３３】

図４は外部バス１４０と内部バス１４１を接続するためのバスインターフェース回路に本発明を適応した構成図を示したものである。

【００３４】

アクセス制御回路１２４は外部バス１４０と内部バス１４１へ接続されており、双方のバス間のデータ転送を行う。アクセス制御回路１２４からアクセス可能であるかどうかを調査するために照会アドレス１４２を用いてＴＬＢ１１１へ接続する。それを受けたＴＬＢ１１１はアクセス可能であるかどうかの合否判定を行い、その結果であるＴＬＢ合否信号１４３と、ＴＬＢ１１１を用いてアドレス変換を行った結果のアドレス１４４をアクセス制御回路１２４へ送る。その結果を用いてアクセス制御回路は内部バス１４１へのリクエストを出力する。また、内部バス１４１を通してのみＴＬＢ１１１は書き換え可能であるため、内部バス１４１からのＴＬＢ更新要求をＴＬＢ制御回路１４７が受け、ＴＬＢ更新信号１

４５とＴＬＢ１１１内のどのエントリを変更するかを通知するアドレスをエントリアドレス１４６を通して、ＴＬＢ１１１へ送る。送られてきたアドレスを元にＴＬＢ１１１内部を更新し、アクセスの制限を行うことが可能となる。

【００３５】

ここで、ＴＬＢ更新要求はプロセッサコア１０１から発行される。また、上記ＴＬＢ更新要求は、アクセス制御回路にも送信されるが、内部バスのアドレスからアクセス制御回路とＴＬＢ制御回路のどちらかへの要求と判断される。

【００３６】

図５は図４とは別の実現方法で本発明を適応した実施例を示したものである。アクセス制御回路１５０は外部バス１５１と内部バス１５２へ接続されており、双方のバス間のデータ転送を行う。許可ビット制御回路１６１は内部バス１５２に接続されたプロセッサコア等からのリクエストを随時受け付けており、外部バス１５１からのアクセスの制限を変更したい場合に要求が送られる。

まず、外部バス１５１からリード、もしくはライトリクエストにより、アドレスがアクセス制御回路１５０とアクセス判定回路１５３内部のアドレスデコーダ１５４へと送られる。アドレスデコーダ１５４へと送られたアドレスにより領域選択信号１５５をセレクタ１５６へ送る。許可ビット群１６０から許可ビット信号１５８、１５９を通してセレクタ１５６へ常に送られている許可ビット信号の一つを領域選択信号１５５により、その一つを選択しアクセス合否信号１５７を通してアクセス制御回路１５０へ結果を送る。ここで、ビット群は、レジスタ群に格納されたビット情報の意である。その信号を受けたアクセス制御回路１５０は要求のあったアドレスに対して破棄するかを決定し、アクセス可能領域であるならば内部バス１５２へリクエストを発生させる。

【００３７】

また、許可ビット群１６０の書き換えは内部バス１５２より発生した書き換え要求を許可ビット制御回路１６１へ送り、その要求によって変更するビットへ許可ビット変更信号１６２、１６３を通して、許可ビット群１６０を変更する。特に、許可ビット群１６０の変更は内部バス１５２からのみ変更可能であり、外部バス１５１からの変更は一切行うことができない。

【００３８】

図６は、アクセス制御のフローチャートである。まず、メディアプロセッサが起動し（４００）、ＴＬＢの設定４０１を行う。ＴＬＢ初期値４０２からデータを読み出し、ＴＬＢの設定を行うが、この初期設定値はフラッシュメモリ等の不揮発性メモリに収められている。ＴＬＢの設定４０１後に、メディアプロセッサは、プログラムの読み込み４０３において、ＴＬＢ初期値４０２同様にフラッシュメモリに収められたプログラム４０４をメディアプロセッサ自身のローカルメモリへ読み出す。

【００３９】

そのプログラムを実行中に外部からのアクセス４０５が発生したかどうかを判定し、発生していない場合はプログラム実行を継続し、発生した場合はＴＬＢの参照４０６を行う。ＴＬＢの参照４０６の結果、許可領域のアクセス４０７であるかどうかを判別し、許可領域ではなかった場合はそのリクエストを破棄し、プログラムの実行を継続し、外部からのアクセス４０５が発生するまで待機する。許可領域のアクセスであった場合にはデータ転送４０８を行い、リードリクエストであればメモリ４０９からデータを読み出し、ライトリクエストであればメモリ４０９へ書き込みを行う。この時のメモリ４０９はローカルメモリや内部メモリ、内部レジスタが対象となる。

【００４０】

ＴＬＢ内部の構造を図７に示す。まず、ＴＬＢ１１１内部の情報を書き換えるため、ＴＬＢ更新信号１１５を受信する。ＴＬＢ更新信号１１５にはＴＬＢエントリデータ３００とＴＬＢアドレス３０１が含まれる。ＴＬＢアドレス３０１の信号はデコーダ３０２に送信され、デコーダ３０２で書き換えるべきＴＬＢ１１１のエントリが確定する。そのアドレスに対して、ＴＬＢエントリデータ３００が書き込まれ、ＴＬＢ１１１の内容である有効ビット３０３、仮想ページ番号３０４、アクセスサイズ３０５が更新される。

【００４１】

更新されたＴＬＢ１１１内の比較器３１０では、外部からのアクセスによるアクセスアドレス３０７とＴＬＢ１１１に格納された内容と比較をする。このとき

、有効ビット３０３は有効ビット信号３１１を通して比較器３１０へ送られ、有効なエントリとのみ比較を行う。有効なエントリの仮想ページ番号３０４は、アクセスが許可されるアドレスの先頭番地を示しており、アクセスサイズ３０５を足した値が終了番地を示している。そのため、これらの信号をそれぞれ仮想ページ番号信号３０８とアクセスサイズ信号３０９として比較器３１０へ送り、アクセスアドレス３０７がその範囲内のアクセスであるか否かを判定し、比較結果３１２をエントリ毎に出力する。

【００４２】

エントリ毎に出力された比較結果３１２はＯＲ回路３１３によって論理和をとり、アクセス判定信号３１４を返す。このような回路によってアクセスの許可、不許可を決定する。

【００４３】

さらにアドレス変換機能を持った場合のＴＬＢ内部の構造を図８に示す。ＴＬＢ１１１内部の情報を書き換えるため、ＴＬＢ更新信号１１５があり、その信号はＴＬＢエントリデータ３００とＴＬＢアドレス３０１の信号である。ＴＬＢアドレス３０１の信号をデコーダ３０２によって書き換えるべきＴＬＢ１１１のエントリが確定する。そのアドレスに対して、ＴＬＢエントリデータ３００が書き込まれ、ＴＬＢ１１１の内容である有効ビット３０３、仮想ページ番号３０４、アクセスサイズ３０５、物理ページ番号３１６が更新される。尚、本実施例では、上記パラメータを更新すべきパラメータとして選択したが、常に上記パラメータの更新を要するものではない。

【００４４】

例えば、有効ビットを選択しない場合は、最初はすべて同じデータを物理ページ番号、アクセスサイズに入れておいて、かつ、アクセスサイズは全領域アクセス可能にすることが考えられる。

【００４５】

また、物理ページ番号、アクセスサイズは、始点、終点を示し、どこからどこまでをアクセスできるかを記述しているが、これらのパラメータを選択しない場合は、物理ページ領域を始点として固定領域をアクセス可能にすることも可能で

ある。

【００４６】

更新されたＴＬＢ１１１は外部からのアクセスによるアクセスアドレス３０７が、比較器３１０でＴＬＢ１１１の内容と比較をする。このとき、有効ビット３０３を有効ビット信号３１１を通して比較器３１０へ送り、有効なエントリとのみ比較を行う。有効なエントリの仮想ページ番号３０４は、アクセスが許可されるアドレスの先頭番地を示しており、アクセスサイズ３０５を足した値が終了番地を示している。そのため、これらの信号をそれぞれ仮想ページ番号信号３０８とアクセスサイズ信号３０９として、比較器３１０へ送り、比較器３１０ではアクセスアドレス３０７がその範囲内をアクセスしているかを判定し、比較結果３１２を各エントリ毎に出力する。この信号はＯＲ回路３１３と、該当するエントリの物理ページ番号を選択するセレクタ３１８へ送られる。ＯＲ回路３１３へ送られた比較結果３１２は論理和をとり、アクセス判定信号３１４を返す。また、セレクタ３１８では、ｎ個ある物理ページ番号（ＰＰＮ）３１６のうちの一つを選択し、変換後アドレス３１９を出力する。この変換は、外部バスからのアクセスが発生した場合、外部バス上のアドレスで行われる。そのアドレスはＴＬＢ１１１を搭載するプロセッサ内部のアドレスとは違うため、アドレスの変換を行う必要がある。このアドレス変換でのボトルネックを解消するために物理ページ番号への変換機能を持たせ、プロセッサ内部をアクセスできるアドレスへ高速に変換することが可能である。

【００４７】

ＴＬＢ１１１にアクセス可能領域、不可領域を設定した場合を図９に示す。ＴＬＢ１１１内のエントリＡ３３０によってローカルメモリ３３４を参照可能領域に設定している。また、エントリＢ３３１によってローカルメモリ３３６を参照可能領域に設定している。ローカルメモリ３３５とローカルメモリ３３７はＴＬＢ１１１によって参照可能領域に設定されていないため、外部からのアクセスは遮断される領域となる。

【００４８】

また、エントリＣ３３２によってコプロセッサ用メモリ３３８の領域を参照す

ることが可能である。しかし、コプロセッサ用メモリ３３９の領域はＴＬＢ１１１によって参照可能領域に設定されていないため、外部からのアクセスは遮断される。同様に、レジスタマップの領域のうち、エントリＤ３３３によってレジスタマップ３４１が参照可能領域となっている。レジスタマップ３４１の前後の空間である、レジスタマップ３４０とレジスタマップ３４２は参照不可領域であり、プロセッサ外部からのアクセスは遮断され、リード、ライトすることができない。

【００４９】

ただし、アクセス不可領域は外部からのアクセスのみ遮断し、プロセッサ内部からは、制限なくアクセスすることができる。

【００５０】

また、図１０にはＰＣＩのベースアドレスレジスタ（以下、ＢＡＲ）を用いてメモリ空間のアクセスできる領域を制限する方法を示す。

【００５１】

まず、ＰＣＩのＢＡＲを用いてメモリ空間のアクセスできる領域を制限する方法の概要を示す。

【００５２】

ＰＣＩデバイスには、そのデバイスが必要とするメモリ空間があり、各デバイスによってそのサイズは様々である。現在のＰＣＩの規格ではＰＣＩは４ＧＢのメモリ空間を持っているが、その空間上に、ＰＣＩデバイスのメモリ空間を割り当てている。例えば、ＰＣＩデバイスＡが0x4000のメモリ空間を持っていたとき、ＰＣＩ空間の0x1000から割り当てると、ＰＣＩバス0x1000～0x4fffをアクセスすると、ＰＣＩデバイスＡのメモリ空間を操作することが可能となる。ここで、該メモリ空間を設定するときに使用するものがＢＡＲであり、デバイス側が必要に応じて自分自身のＢＡＲのサイズを変更できるようにするものである。具体的には、ＰＣＩデバイスは128MBのメモリを持っていたとき、本来、ＰＣＩ空間には128MB分の空間を割り当てることができる。しかし、故意に64MBしか割り当てないようにする（実現方法は図１０、１１）ことで、ＰＣＩから残りの64MBを見えないようにすることができる。

【００５３】

例えば、ＰＣＩバス上にリクエストが発生したとき、各ＰＣＩデバイスはそのリクエストのアドレスをＢＡＲの内容と比較し、そのアドレスが自分宛と判断したときに返答をする。つまり、ＰＣＩデバイスのＰＣＩインターフェースは設定されたＢＡＲとリクエストアドレスを比較し、自分のメモリ空間へのアクセスかを判定している。しかし、ＢＡＲがあらかじめ64MBしかないと設定されていれば、65MBのアクセスがきたとしても、自分へのアクセスではないと判断する。

【００５４】

次に、ＰＣＩのＢＡＲを用いてメモリ空間のアクセスできる領域を制限する具体的な方法を示す。

プロセッサの外部より入力されるＢＡＲの領域を指定するＢＡＲ設定信号３５０が、電源が投入、もしくはソフトウェアリセットや外部リセットボタンによるリセットが発生した場合等にデータ保持レジスタ３５４によって保持される。リセット信号３５１が論理値１の時にリセット期間であることを表す場合、クロック信号３５３とともにＡＮＤ回路３５２に入力して論理積をとり、リセット信号３５１が論理値１を取ったときにデータ保持レジスタ３５４を更新する。保持データ３５５はデコーダ３５６によってＢＡＲへ送るデータが確定する。

【００５５】

確定した信号は、ＢＡＲ３６３のｎビット目３６４、ｎ＋１ビット目３６５、ｎ＋２ビット目３６６、ｎ＋３ビット目３６７用にそれぞれデコード結果３５８、３５９、３６０、３６１をＡＮＤ回路３６２へ送る。それらの信号とＢＡＲ変更信号３５７と論理積がとられ、その結果がＢＡＲ３６３のｎビット目３６４、ｎ＋１ビット目３６５、ｎ＋２ビット目３６６、ｎ＋３ビット目３６７に反映される。

【００５６】

この図１０の方法の場合、デコーダ３５６からデコード結果３５８、３５９、３６０、３６１へ全て論理値１が出力されていた場合、ＢＡＲ変更信号３５７によってｎビット目３６４を含めた上位のビットは変更することが可能である。この領域は、ＰＣＩ空間へ割り当てられる最小領域であり、メモリ空間は２＾ｎを

持つこととなる。このようにして、ＰＣＩ空間へ最大２＾（ｎ＋３）の領域を割り当てることが可能である。このような設定ができるプロセッサにおいて２＾（ｎ＋３）のローカルメモリを持っていたとして、ＢＡＲへ２＾ｎを設定できるようにする。この場合、番地０～（２＾ｎ－１）まではＰＣＩ空間から参照可能であるが、番地（２＾ｎ）～（２＾（ｎ＋３）－１）まではＰＣＩ空間に割り当てられないため、外部のデバイスからは不可視となり、アクセスすることはできない。このような方法を用いてアクセスを抑制することができる。

【００５７】

図１０のデータ保持レジスタ３５４をプロセッサ内部から変更する場合を図１１に示す。セレクタ３６９を用いて選択信号３７０によって、データ保持レジスタ３５４かプロセッサ内部からのＢＡＲ領域を指定するＢＡＲ設定信号３６８を選択する。選択したデータを再度データ保持レジスタ３５４を更新する。保持データ３５５はデコーダ３５６によってＢＡＲへ送るデータが確定する。確定した信号は、ＢＡＲ３６３のｎビット目３６４、ｎ＋１ビット目３６５、ｎ＋２ビット目３６６、ｎ＋３ビット目３６７用にそれぞれデコード結果３５８、３５９、３６０、３６１をＡＮＤ回路３６２へ送る。それらの信号とＢＡＲ変更信号３５７と論理積がとられ、その結果がＢＡＲ３６３のｎビット目３６４、ｎ＋１ビット目３６５、ｎ＋２ビット目３６６、ｎ＋３ビット目３６７に反映される。

【００５８】

つまり、ベース・アドレス・レジスタのある特定のビットを論理値０固定する機能を有するＰＣＩバスインターフェースにおいて、ある特定のベース・アドレス・レジスタのビットを論理値０固定にすることで、ＰＣＩデバイスが持つローカルメモリよりも小さいメモリ空間を、ＰＣＩバス上のメモリ空間へ割り当て、ローカルメモリを持つＰＣＩデバイス自身は全空間にアクセスすることが可能であるが、それ以外のＰＣＩデバイスはＰＣＩバス上のメモリ空間へ割り当てた小さいメモリ空間にのみアクセスできる。

【００５９】

このような方法によってもＢＡＲを変更することが可能であり、アクセス不可領域を指定することが可能である。

【００６０】

本発明を採用したメディアプロセッサを搭載したセット・トップ・ボックス（以下、ＳＴＢ）を図１２に示す。

【００６１】

ＳＴＢ３８０は、メディアプロセッサ１００と、ローカルメモリバス２００を用いてローカルメモリ２０１、フラッシュメモリバス２０２を用いてフラッシュメモリ２０３、汎用バス３８１を用いてサービスポート３８２が接続、搭載されている。また、本システムはＳＴＢであるため、映像信号の入出力を行うビデオ入出力３８６、音声信号の入出力を行うオーディオ入出力３８７、映像信号の解読などに使用する暗号鍵を保持する暗号記憶カードインターフェース信号３８８、外部の記憶装置と高速にデータ通信を行うための高速デジタルバス３８９、ＢＳデジタルチューナから映像信号を受けるトランスポート・ストリーム・インターフェース信号３９０を持つ。

【００６２】

また、サービスポート３８２は故障診断時に保守端末３９１を接続するためのものであり、サービスポート３８２と汎用インターフェース信号３８３を用いて接続する。汎用インターフェース信号３８３は保守用プロセッサ３９２と接続されており、保守プロセッサ自身もローカルメモリバス３９３を用いてローカルメモリ３９４が接続されている。

【００６３】

保守端末３９１が接続された場合には、ＳＴＢ内部のメモリがリード、ライトできる状態ではなく、ローカルメモリ上のアクセス可能領域３８５のみ、読み書き可能である。ローカルメモリ上のアクセス不可領域３８４はＳＴＢ３８０に搭載されているメディアプロセッサ１００からのみアクセス可能であり、保守を行う場合はアクセス可能領域３８５を用いてメディアプロセッサ１００と通信を行うこととなる。

【００６４】

このため、保守端末以外がサービスポート３８２へ接続され、メディアプロセッサ１００内の重要なデータである、暗号解読に使用する暗号鍵や、メディアプ

ロセッサ１００を動作させるソフトウェアを保護することが可能である。

【００６５】

また、外部からの不正なアクセスにより、メディアプロセッサ内部の機密事項である暗号鍵やソフトウェアが格納されているメモリへのアクセスを遮断することができ、そのアクセス範囲はアプリケーションによって自由に変更可能である。尚、本実施例でアクセス制限がかかるのは物理的な領域であるが、論理的な領域について制限をかけてもよい。　本発明は、上述の実施の形態に限定されるものではなく、適用分野に関わらず、要旨を逸脱しない範囲で変更し実施し得ることは述べるまでもない。

【００６６】

【発明の効果】

本発明を適用することで、プロセッサ内部の機密情報や、プロセッサに接続するローカルメモリやフラッシュメモリなど外部メモリの内容を保護し、外部からの不正読み出しを防止することが可能となる。

【図面の簡単な説明】

【図１】

本発明を搭載したメディアプロセッサをＰＣＩバスへ接続した構成図である。

【図２】

本発明を搭載したメディアプロセッサを汎用バスへ接続した構成図である。

【図３】

本発明を搭載したＤＳＰを汎用バスへ接続した構成図である。

【図４】

外部バスと内部バスをＴＬＢを用いて接続する構成図である。

【図５】

外部バスと内部バスをアクセス制御ビット群を用いて接続する構成図である。

【図６】

アクセス制御のフローチャート図である。

【図７】

ＴＬＢ内部の構成図である。

【図８】

ＴＬＢにアドレス変換機能を持ったＴＬＢ内部の構成図である。

【図９】

メモリやレジスタマップへの割り当てを示す図である。

【図１０】

ＢＡＲを用いたアクセス制御の構成図である。

【図１１】

ＢＡＲを用いたアクセス制御の構成図である。

【図１２】

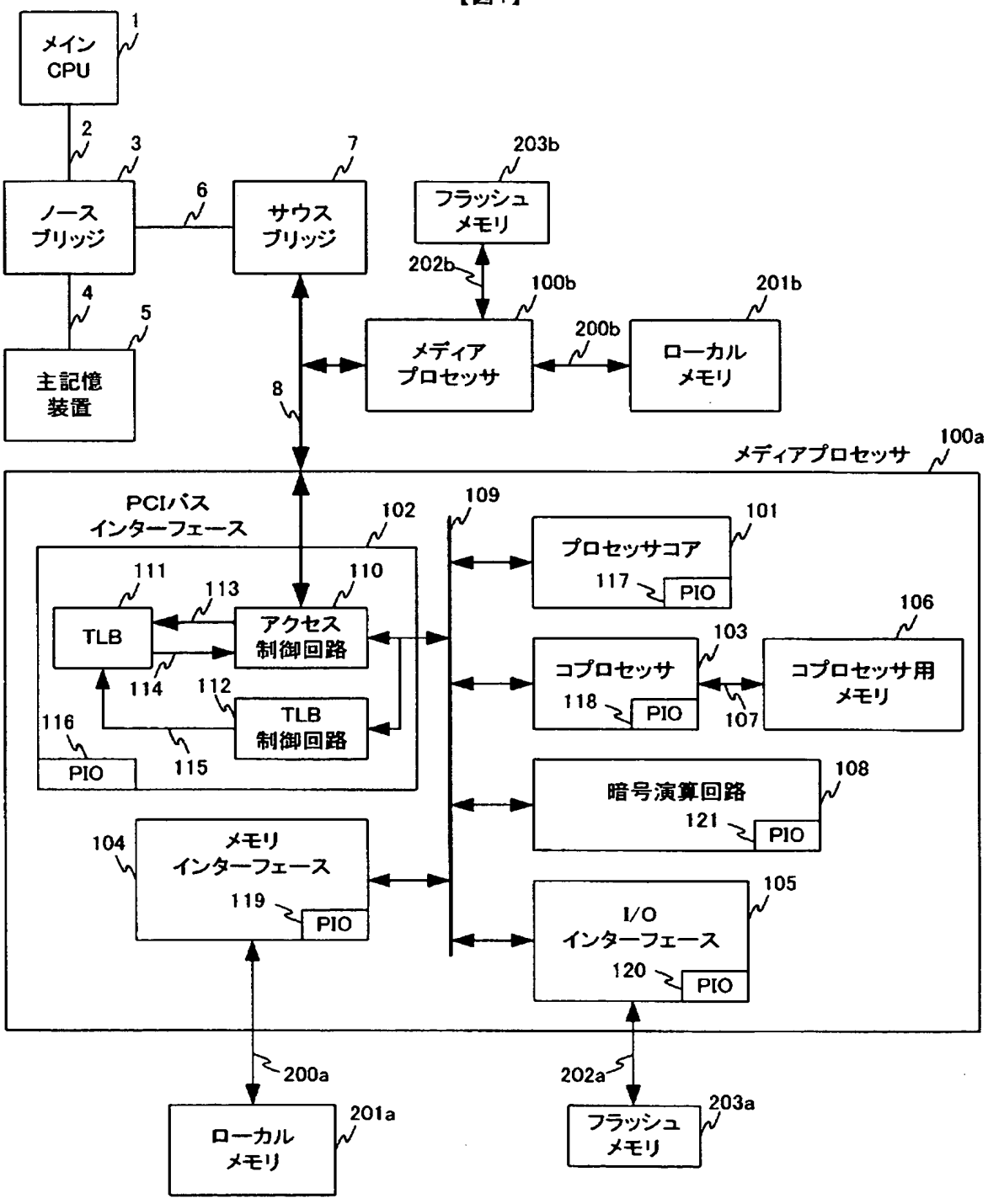
本発明を搭載したメディアプロセッサをＳＴＢに用いた構成図である。

【符号の説明】

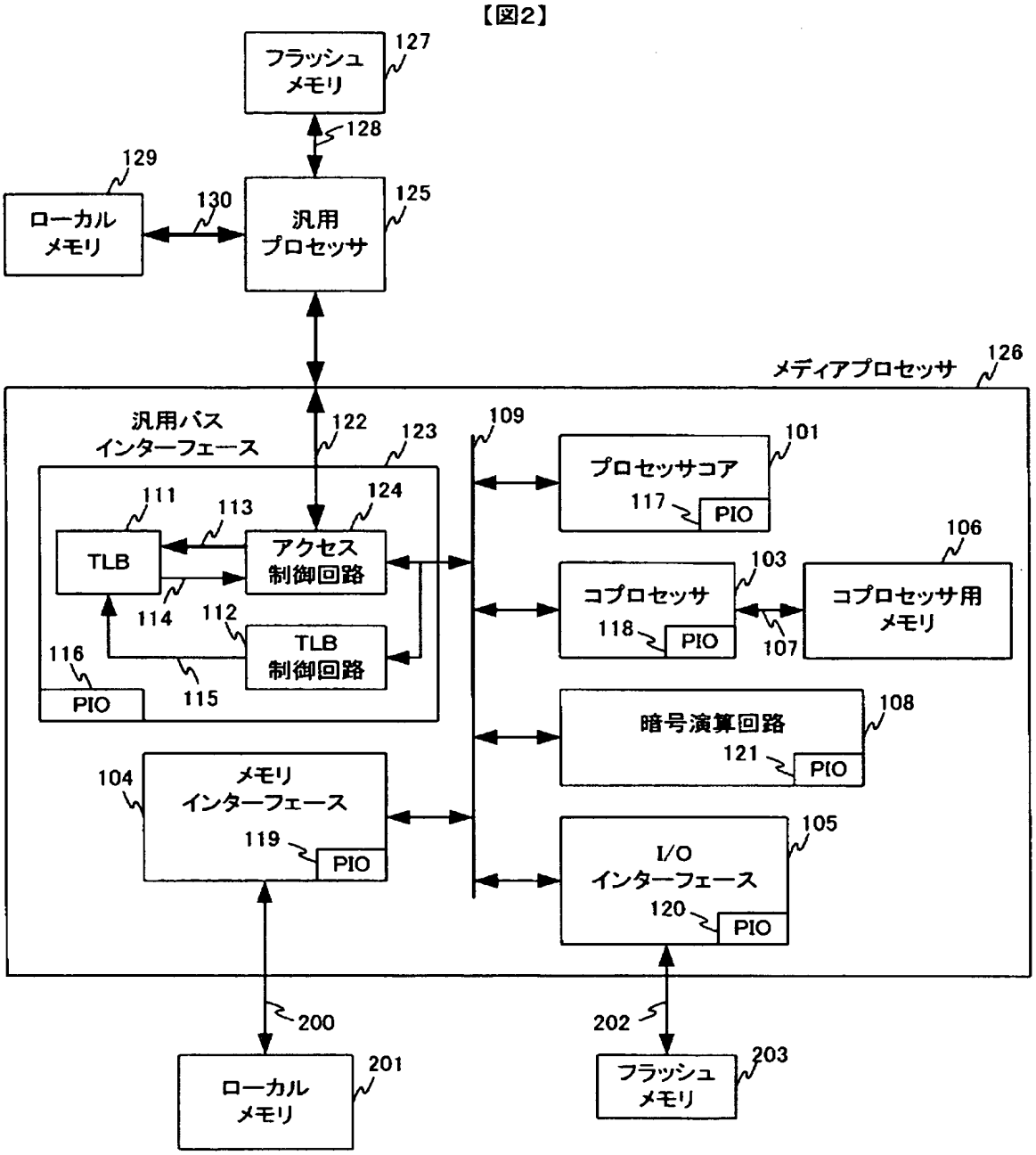
１…メインＣＰＵ、３…ノースブリッジ、５…主記憶装置、７…サウスブリッジ、１００…メディアプロセッサ、１０１…プロセッサコア、１０２…ＰＣＩバスインターフェース、１１０…アクセス制御回路、１１１…ＴＬＢ、１１２…ＴＬＢ制御回路、１２５…汎用プロセッサ、１３１…デジタルシグナルプロセッサ、２０１…ローカルメモリ、２０３…フラッシュメモリ、３０３…有効ビット、３０４…仮想ページ番号、３０５…アクセスサイズ、３１６…物理ページ番号

【書類名】図面

【図１】

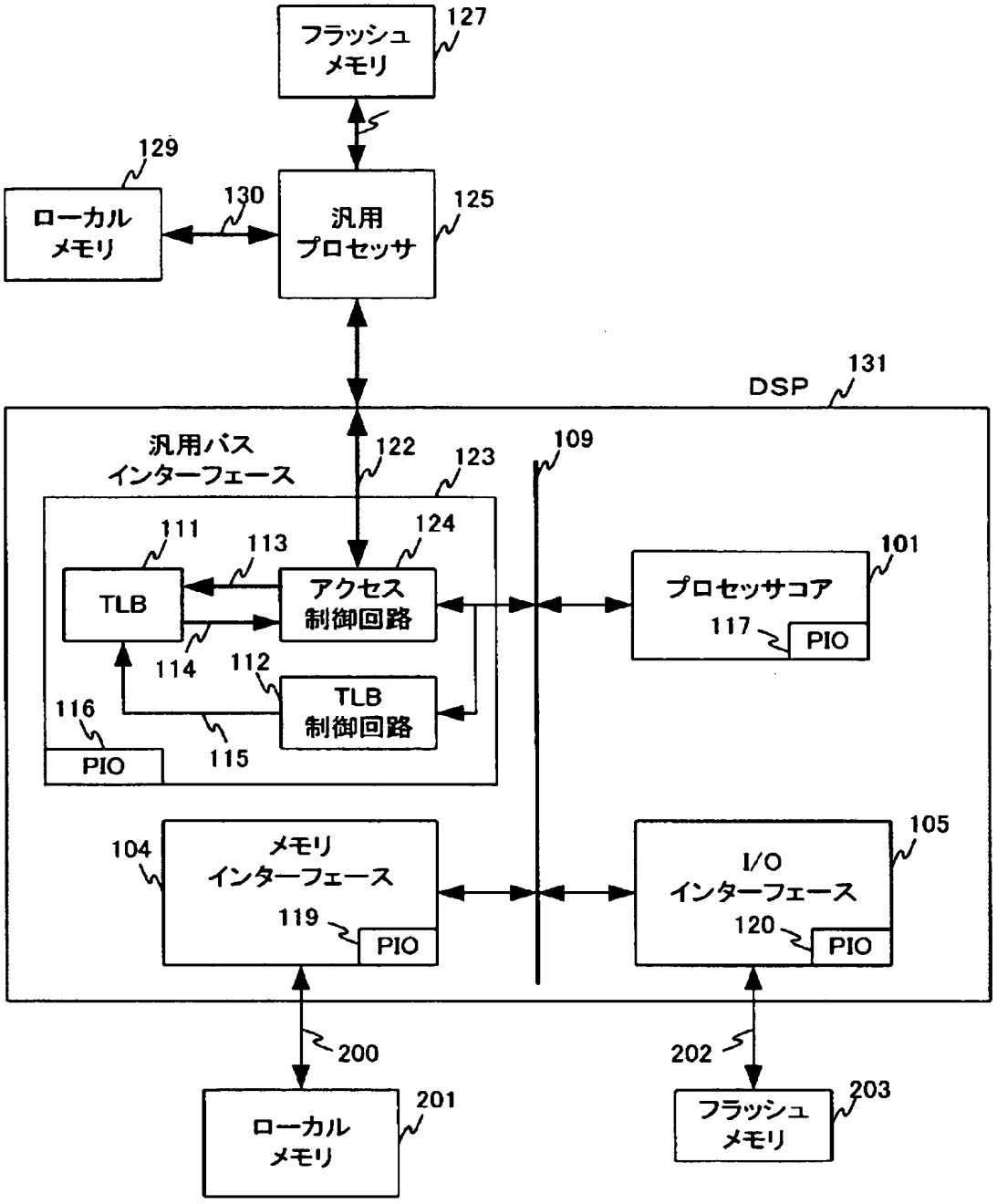

【図1】
メイン CPU
1
2
3
ノース ブリッジ
6
サウス ブリッジ
7
203b
フラッシュ メモリ
202b
100b
201b
4
5
主記憶 装置
メディア プロセッサ
200b
ローカル メモリ
8
100a
メディアプロセッサ
PCIバス インターフェース
102
109
101
プロセッサコア
117
PIO
111
113
110
TLB
アクセス 制御回路
106
103
コプロセッサ
118
PIO
コプロセッサ用 メモリ
107
114
112
TLB 制御回路
116
115
PIO
108
暗号演算回路
121
PIO
104
メモリ インターフェース
119
PIO
105
I/O インターフェース
120
PIO
200a
202a
ローカル メモリ
201a
フラッシュ メモリ
203a

【図２】


【図2】
フラッシュメモリ
127
128
129
ローカルメモリ
130
汎用プロセッサ
125
メディアプロセッサ
126
汎用バスインターフェース
122
123
109
プロセッサコア
101
117
PIO
111
113
124
TLB
アクセス制御回路
106
103
コプロセッサ
コプロセッサ用メモリ
118
PIO
107
114
112
TLB制御回路
116
PIO
115
暗号演算回路
108
121
PIO
104
メモリインターフェース
119
PIO
I/Oインターフェース
105
120
PIO
200
202
ローカルメモリ
201
フラッシュメモリ
203

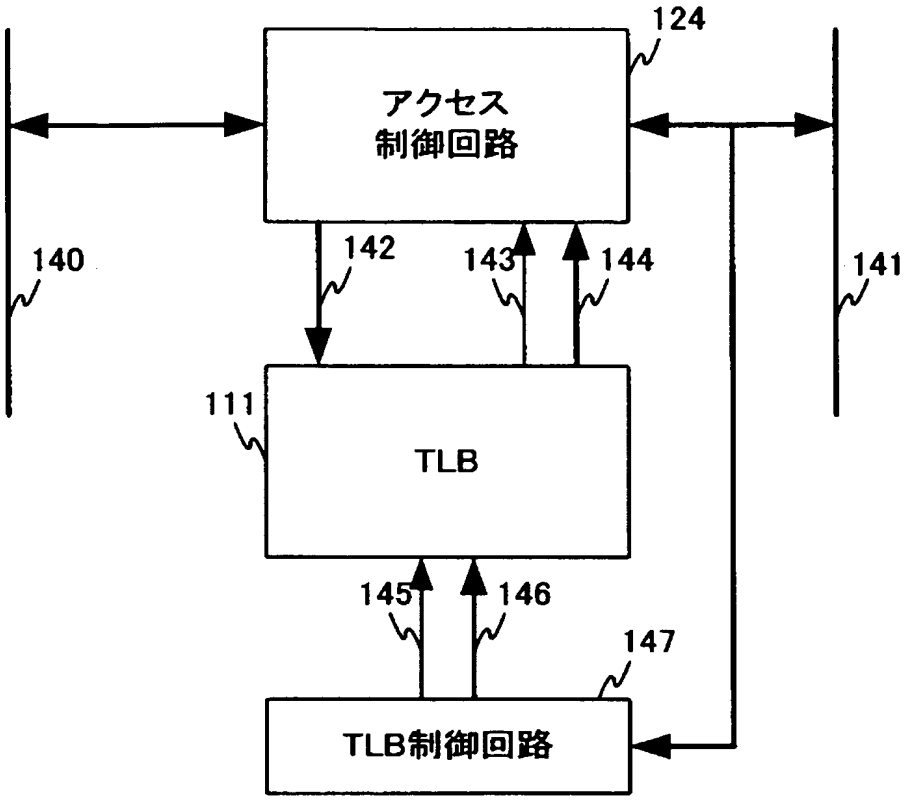
【図３】

【図3】


フラッシュ
メモリ
127
129
ローカル
メモリ
130
汎用
プロセッサ
125
DSP
131
汎用バス
インターフェース
122
123
109
111
113
124
TLB
アクセス
制御回路
101
プロセッサコア
117
PIO
114
112
TLB
制御回路
116
PIO
115
104
メモリ
インターフェース
119
PIO
105
I/O
インターフェース
120
PIO
200
202
201
ローカル
メモリ
203
フラッシュ
メモリ

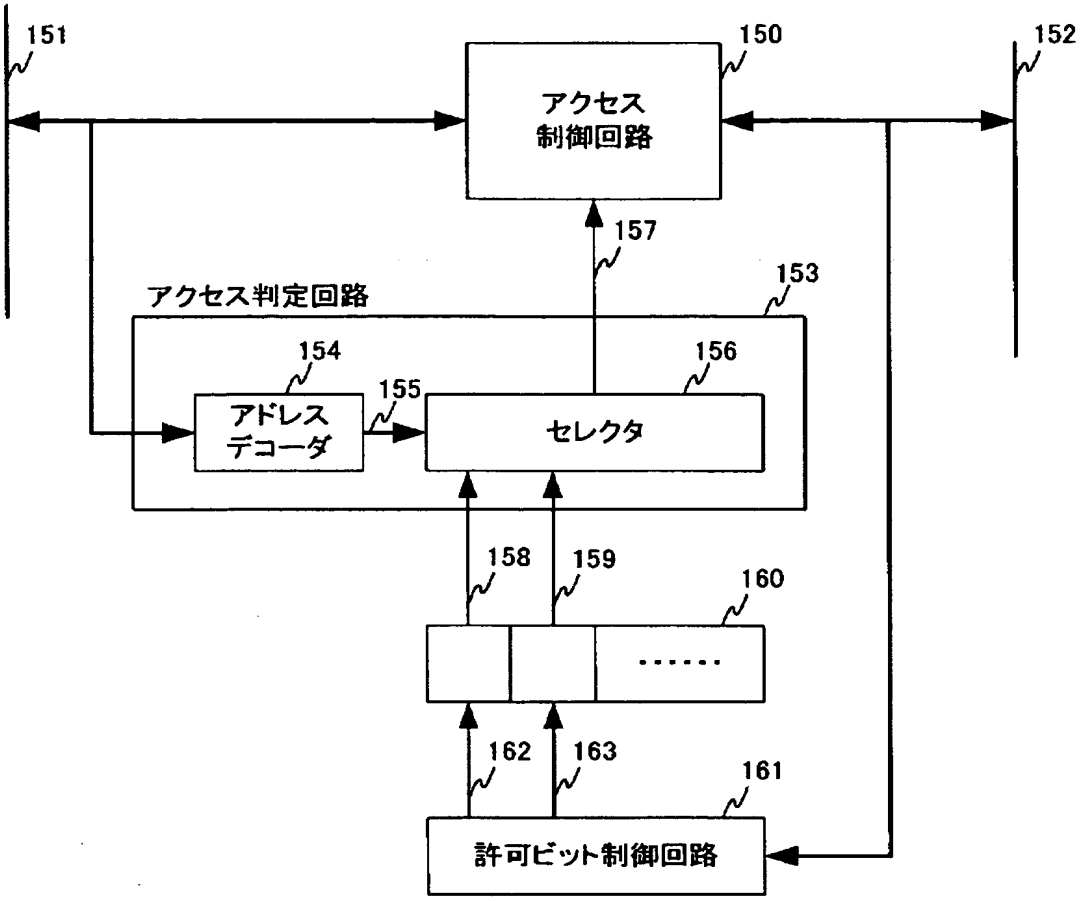
【図４】

【図4】

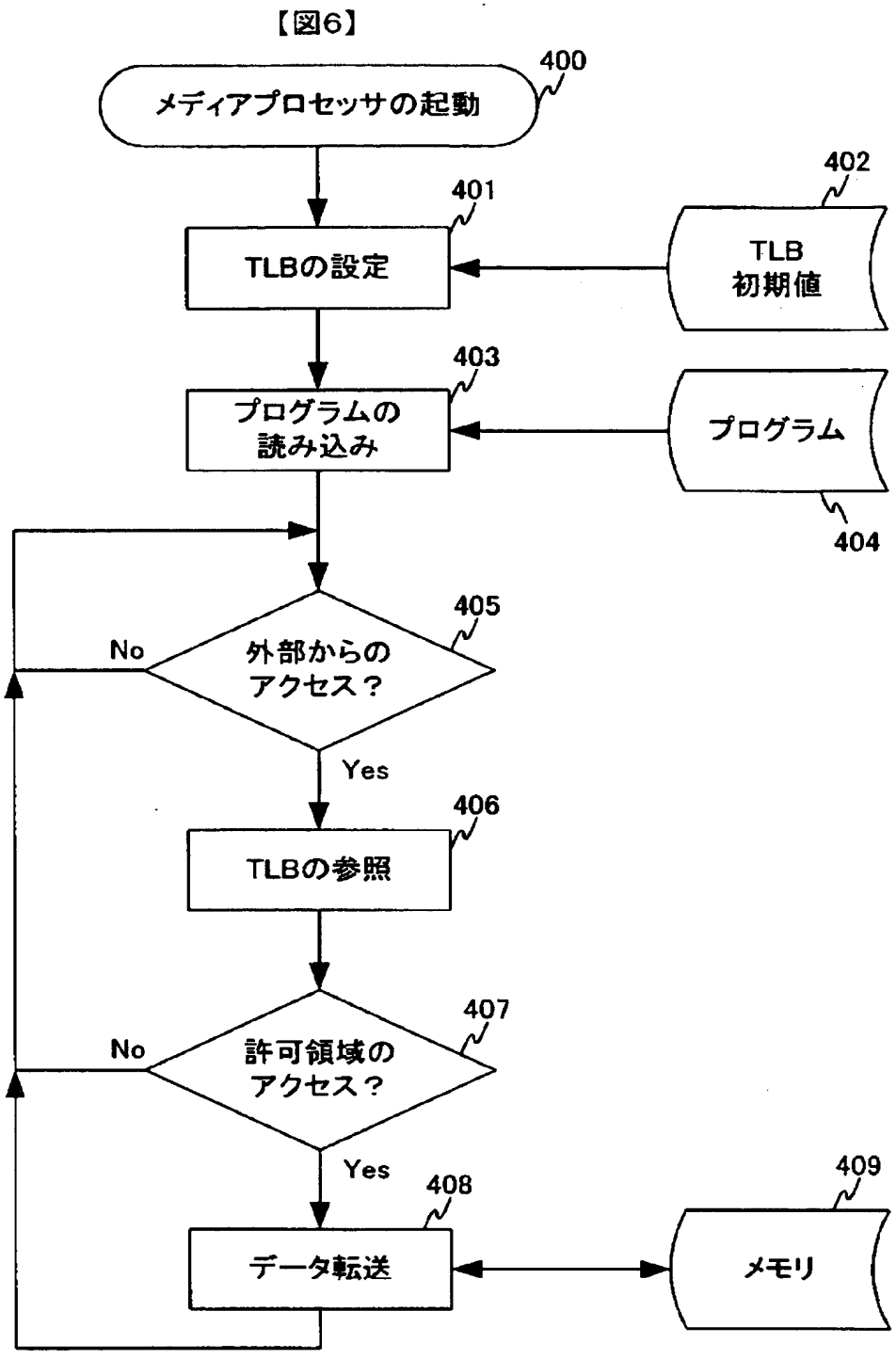


【図５】

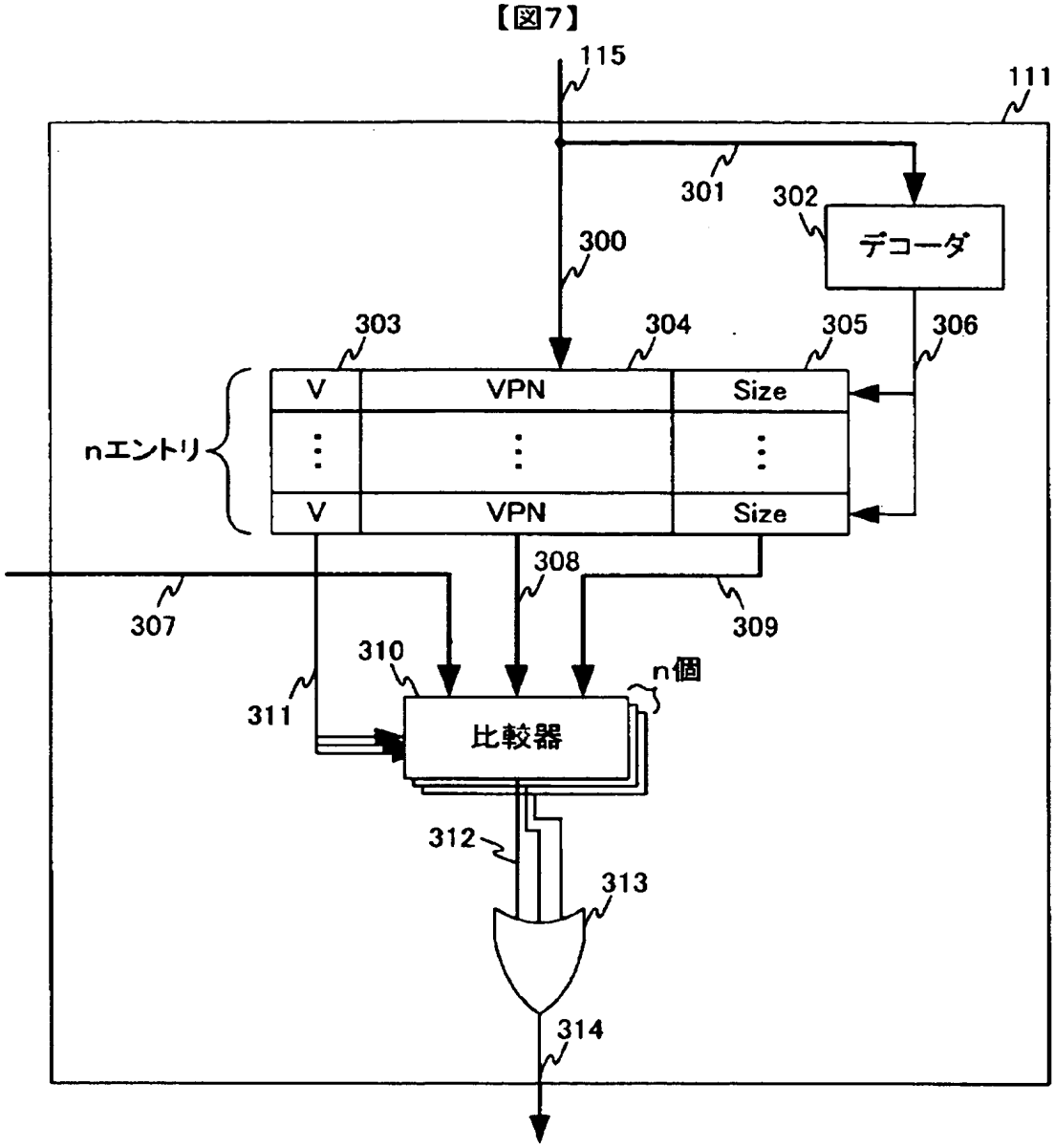
【図5】


151
150
152
アクセス
制御回路
157
153
アクセス判定回路
154
156
155
アドレス
デコーダ
セレクタ
158
159
160
162
163
161
許可ビット制御回路

【図６】

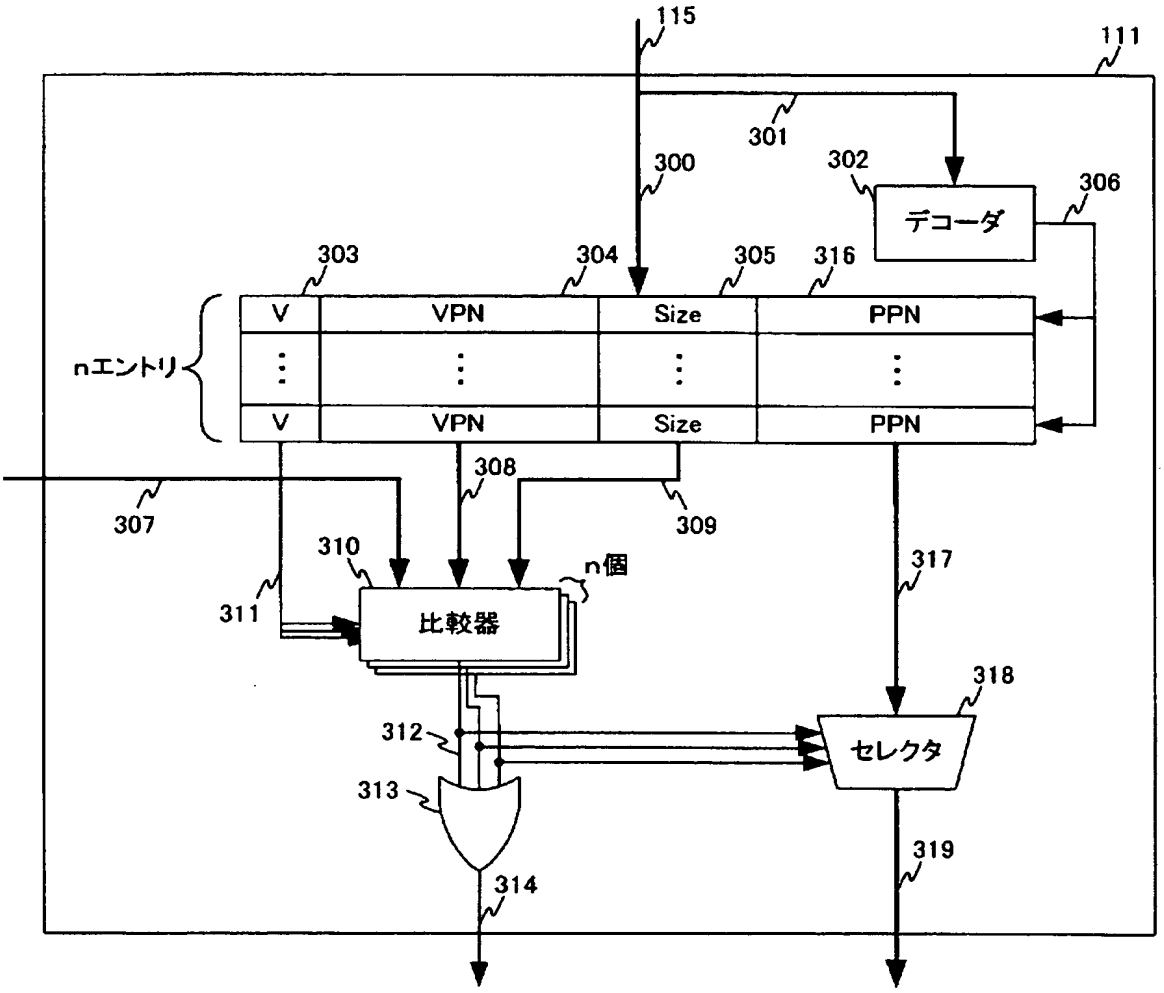

【図6】
400
メディアプロセッサの起動
401
TLBの設定
402
TLB
初期値
403
プログラムの
読み込み
プログラム
404
405
No
外部からの
アクセス？
Yes
406
TLBの参照
407
No
許可領域の
アクセス？
Yes
408
データ転送
409
メモリ

【図７】

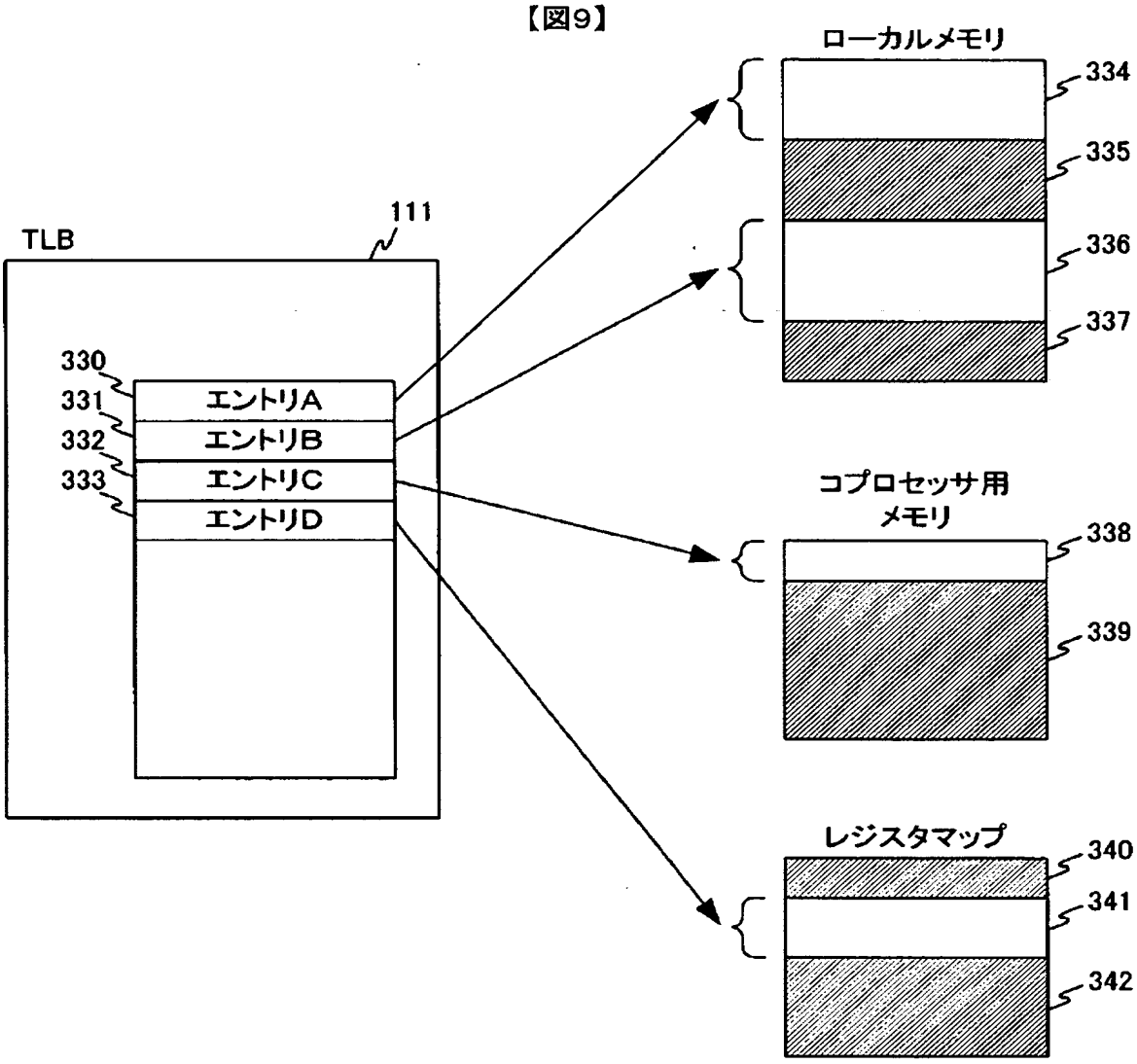

【図7】
115
111
301
302
デコーダ
300
303
304
305
306
V
VPN
Size
nエントリ
V
VPN
Size
308
307
309
310
n個
311
比較器
312
313
314

【図８】

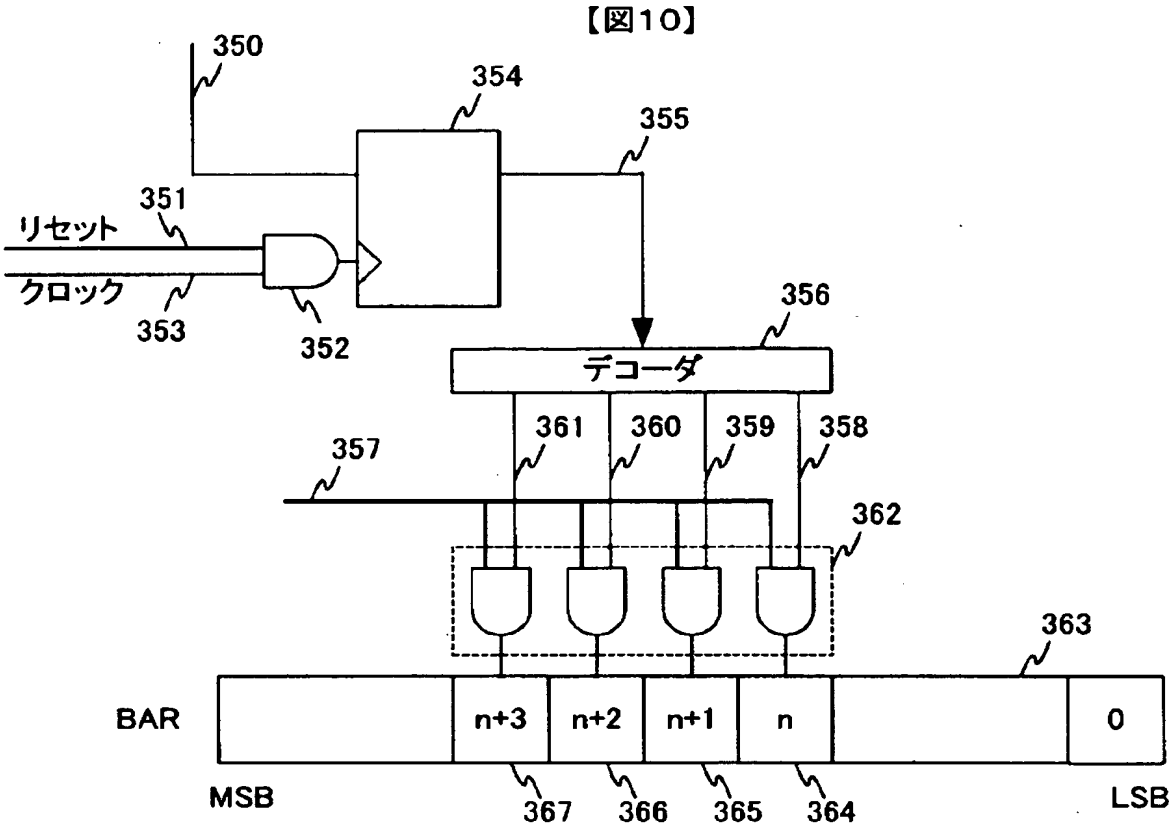
【図8】


115
111
301
300
302
306
デコーダ
303
304
305
316
V
VPN
Size
PPN
nエントリ
V
VPN
Size
PPN
308
307
309
310
n個
311
比較器
317
318
312
セレクタ
313
319
314

【図９】

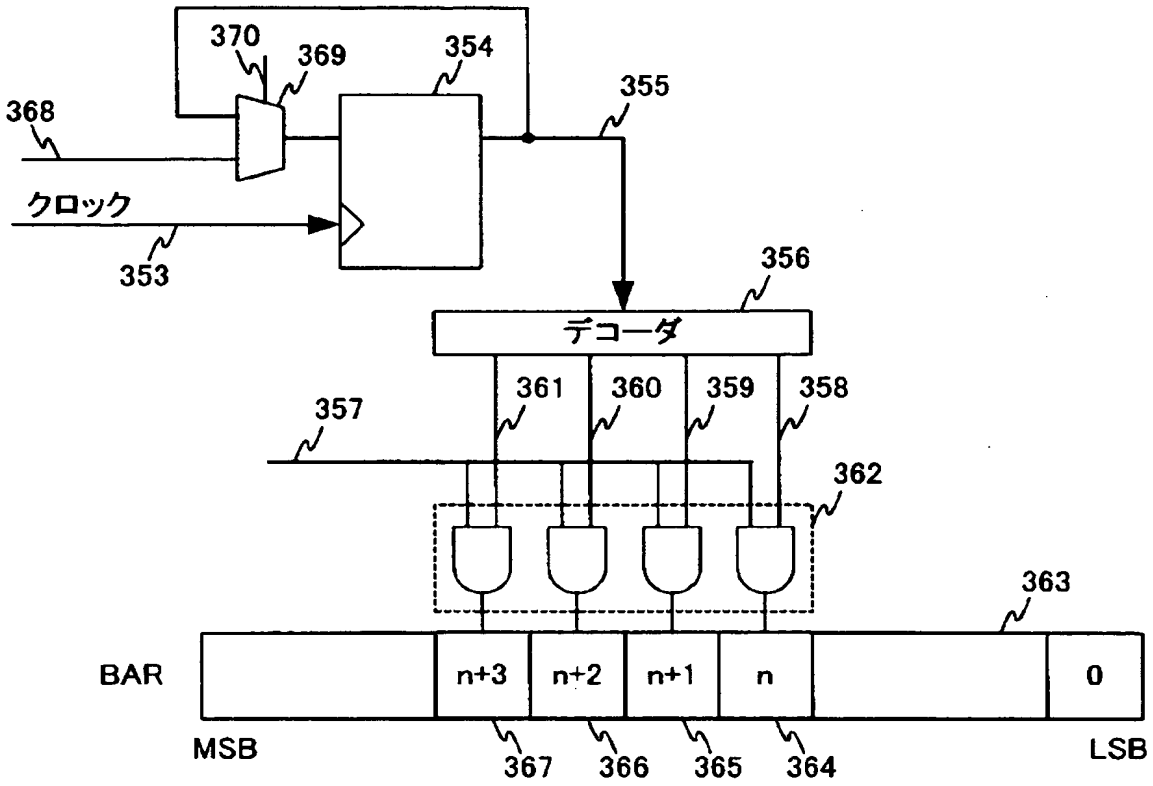

【図9】
ローカルメモリ
334
335
336
337
111
TLB
330
331
332
333
エントリA
エントリB
エントリC
エントリD
コプロセッサ用
メモリ
338
339
レジスタマップ
340
341
342

【図１０】


【図10】
350
354
355
351
リセット
クロック
353
352
356
デコーダ
361
360
359
358
357
362
363
BAR
n+3
n+2
n+1
n
0
MSB
LSB
367
366
365
364

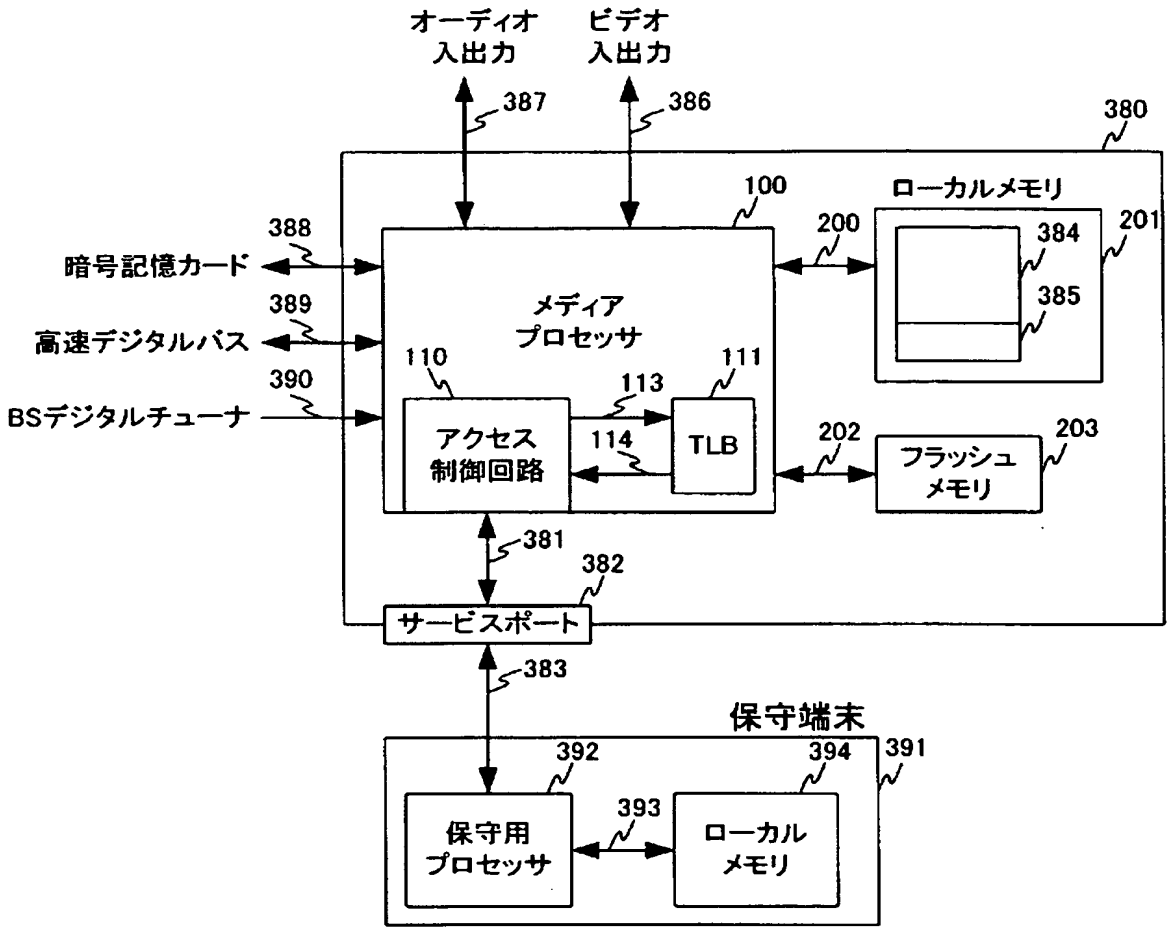
【図１１】

【図11】


370
369
354
355
368
クロック
353
356
デコーダ
361
360
359
358
357
362
363
BAR
n+3
n+2
n+1
n
0
MSB
LSB
367
366
365
364

【図１２】

【図12】


オーディオ
入出力
ビデオ
入出力
387
386
380
100
ローカルメモリ
200
201
384
385
388
暗号記憶カード
389
高速デジタルバス
390
BSデジタルチューナ
メディア
プロセッサ
110
111
113
114
アクセス
制御回路
TLB
202
203
フラッシュ
メモリ
381
382
サービスポート
383
保守端末
392
394
391
393
保守用
プロセッサ
ローカル
メモリ

【書類名】要約書

【要約】

【課題】

外部バスからプロセッサ内部のレジスタやローカルメモリの読み出しや改変が可能であった。そのため、暗号鍵などの機密データが読み出されたり、開発したソフトウェアがコピーされてしまう可能性があった。

【解決手段】

外部と接続するバスを持つメディアプロセッサにおいて、外部バスに接続された他のデバイスからのアクセスは全て許可される。そのため、プロセッサ内部の機密事項を保護するために、メディアプロセッサのバスインターフェース部分にＴＬＢを設け、そのＴＬＢはプロセッサ内部からのみ書き換えることができる。このＴＬＢは外部からアクセスされたアドレスが、アクセスできるかを判定する。ＴＬＢ内にアクセス許可が記述されていればメディアプロセッサ内部へアクセスを発生し、そうでなければリクエストを破棄する。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００３－０７２９１９
受付番号	５０３００４３６５３７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　３月１９日

＜認定情報・付加情報＞

【提出日】　平成15年 3月18日

次頁無

【書類名】　出願人名義変更届（一般承継）

【あて先】　特許庁長官　殿

【事件の表示】

【出願番号】　特願2003- 72919

【承継人】

【識別番号】　503121103

【氏名又は名称】　株式会社ルネサステクノロジ

【承継人代理人】

【識別番号】　100080001

【弁理士】

【氏名又は名称】　筒井　大和

【提出物件の目録】

【包括委任状番号】　0308729

【物件名】　承継人であることを証明する登記簿謄本　1

【援用の表示】　特許第３１５４５４２号　平成１５年４月１１日付け提出の会社分割による特許権移転登録申請書　を援用する

【物件名】　権利の承継を証明する承継証明書　1

【援用の表示】　特願平１－２５１８８９号　同日提出の出願人名義変更届（一般承継）を援用する

【プルーフの要否】　要

認定・付加情報

特許出願の番号	特願２００３－０７２９１９
受付番号	５０３０１４０３５２５
書類名	出願人名義変更届（一般承継）
担当官	伊藤　雅美　　２１３２
作成日	平成１５年１１月　４日

＜認定情報・付加情報＞

【提出日】　平成15年 8月26日

特願２００３－０７２９１９

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所

特願２００３－０７２９１９

出　願　人　履　歴　情　報

識別番号　　［５０３１２１１０３］

１．変更年月日　　２００３年　４月　１日
［変更理由］　　新規登録
住　所　　東京都千代田区丸の内二丁目４番１号
氏　名　　株式会社ルネサステクノロジ